COLORTOKENS

Use Case Analysis

PCI Compliance

Cardholder Data is Everywhere

Achieving PCI DSS compliance is a tremendous challenge. Cardholder data is processed and stored in many different places, from systems in data centers and on cloud platforms, to point of sale (POS) systems, PCs, and kiosks in stores. PCI violations are spiking, leading to damaged brand reputations and increased fines. Standards are tightening in areas like POS security and controlling administrative access to the cardholder data environment (CDE).

That's why meeting PCI requirements can seem like a never-ending struggle. IT organizations must find every place cardholder data resides and restrict access to people and applications with a demonstrated "need to know." Then they need to monitor all access and prove to auditors that they are in full compliance.

ColorTokens Xtended ZeroTrust Platform offers a single security solution that enables IT teams to understand exactly where cardholder data flows, minimize access by users and applications, and scan their environment for vulnerabilities and unprotect paths to confidential data. It helps them protect against unpatchable vulnerabilities, respond to threats faster, and streamline audits.

Challenges

- Understand the scope of systems that process and store cardholder data
- Document all the users and applications that access CDEs
- Restrict access to CDEs by business need to know
- Apply PCI rules in dynamic cloud environments where enterprises have little control
- Minimize the "blast radius" of compromises

Requirements

- Discover all systems that process and store cardholder data
- Microsegment CDEs from unauthorized users and applications
- Protect unpatched POS systems and remote PCs from malware
- Ease the burden of proving compliance to auditors with out-of-the box reports and real-time network maps

Reducing Risk Across the Board

Visibility into systems and paths that expose your cardholder data

Xview for Visibility, part of the Xtended ZeroTrust Platform, discovers application workloads running in virtual machines and containers on premises and on cloud platforms. You can tag each workload with information such as the application it belongs to, the platform it runs on (such as VMWare, AWS, Azure, or Google Cloud), and whether it is part of a CDE.

Xview then creates a comprehensive network map of all the workloads and the connections between them and connections to domains across the web. With this comprehensive map, you can see how application workloads interact, and their dependencies.

Xview identifies paths for lateral movement that advanced attacks can use to reach cardholder data. The vulnerability scanner highlights the most exposed systems in CDEs, so you can give priority to monitoring them for vulnerabilities and indicators of attack. It also simplifies internal firewall traffic audits, uncovers misconfigured ports, and highlights unauthorized connections that violate PCI and other regulations.

Microsegmentation to isolate CDEs

Xshield for Workload Protection and Microsegmentation, another part of the Xtended ZeroTrust Platform, enables you to isolate CDEs and protect cardholder data by blocking traffic to and from unauthorized systems and users. It provides an automated and auditable process to create, monitor, and enforce policies that restrict access to each application workload to users and applications with a "business need to know" as defined by the PCI standards.

Once policies are assigned to a workload, Xshield ensures that they are applied to every instance of that workload on every cloud platform and in every data center, regardless of the underlying technology. When virtual environments move an instance of a workload, the security policies move with them. The effect of policies can be simulated and refined in a non-blocking "observe" mode, and deployed policies can be rolled back if necessary.

Endpoint lock-down and encryption for POS systems

Xprotect for Endpoint Detect and Response, the third part of the Xtended ZeroTrust Platform, can lock down POS terminals, PCs, and kiosks in geographically dispersed locations, making them tamper-proof. Application modules and services not on the whitelist for that device simply will not execute. Systems that process or store cardholder data are protected from malware, including fileless malware and zero-day threats.

Xprotect even preserves the integrity of legacy systems and specialized devices that are difficult or impossible to patch.

Xprotect also supports PCI compliance by providing one-click AES 256-bit encryption of data in motion between protected devices and central servers.

Accelerated incident response

The Xtended ZeroTrust Platform can detect attempts by unauthorized users and systems to access CDE application workloads on cloud platforms and in data centers. It can also highlight anomalous traffic flows into and out of CDEs, alerting incident response teams and providing information on the outside system. The team can then use Xshield to block the suspicious traffic immediately, before cardholder data is lost.

Limiting the scope of audits and the burden of compliance

A PCI audit can be costly. The Xtended ZeroTrust Platform can reduce those costs by providing the data to narrow the scope of the audit to just those systems that actually process and store cardholder data in the data center and remote locations. It also generates reports and networks maps that show auditors how the organization is restricting access to cardholder data and complying with other PCI DSS requirements, eliminating the need to compile and document thousands of firewall rules and ACL lists.

Results

With ColorTokens Xtended ZeroTrust Platform you can:

- **Discover systems that process cardholder data** in on-premises data centers and on cloud platforms
- **Reduce risks** by identifying paths for lateral movement into CDEs, exposed workloads, misconfigured ports, and unauthorized connections
- **Implement micro-segmentation** to isolate and protect CDEs
- **Assign to application workloads** access policies that enforce PCI requirements
- **Follow the workloads** across virtual and cloud environments
- **Lock down endpoints and legacy, POS, and unpatchable systems** to protect them from fileless malware and zero-day attacks, even when they can't be patched
- **Reduce the burden of compliance** by narrowing the scope of audits

ColorTokens Inc., a leader in cloud-delivered ZeroTrust security, provides a modern and new-generation of security that empowers global enterprises with a proactive approach to single-handedly secure cloud workloads, dynamic applications, endpoints and users. Through its award-winning Xtended ZeroTrust Platform, ColorTokens delivers the only cloud-based solution that combines AV, EDR, workload protection and application control into one ultra-lightweight agent. This enables enterprises to instantly visualize and segment their entire IT infrastructure, block advanced malware, contain and respond to APTs and zero-day attacks—all while seamlessly integrating with existing security tools.

colortokens.com
sales@colortokens.com